CLAIMS:

1. A method for cryptographically converting an input data block into an output data block; the method including performing a non-linear operation on the input data block using an S-box based on a permutation, wherein the method includes each time before using the S-box (pseudo-)randomly selecting the permutation from a predetermined set of at least two permutations associated with the S-box.

2. A method as claimed in claim 1, wherein the set of permutations is formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set.

3. A method as claimed in claim 1, wherein the data block consists of n data bits and each element of the set of permutations is a permutation on a set of 2^n elements, represented by $\mathbf{Z}_2^n$, where each non-trivial differential characteristic of each permutation in this set has a probability of at most p_{diff}; the set of permutations being formed by permutations which have been selected such that for each non-trivial differential characteristic with probability of p_{diff} in any of the permutations, this differential characteristic has a probability lower than p_{diff} in at least one of the other permutations of the set.

4. A method as claimed in claim 3, wherein the differential characteristic has a probability equal to zero in at least one of the permutations.

5. A method as claimed in claim 4, wherein $n = 4$, and $p_{diff} = ¼$.

6. A method as claimed in claim 1, wherein the data block consists of n data bits and each element of the set of permutations is a permutation on a set of 2^n elements, represented by $\mathbf{Z}_2^n$, where each non-trivial linear characteristic of each permutation in this set has a probability of at least ½ - p_{lin} and at most ½ + p_{lin}, the set of permutations being formed

by permutations which have been selected such that for each non-trivial linear characteristic with probability of ½ - p_{lin} or ½ + p_{lin} in any of the permutations, this linear characteristic has a probability closer to ½ in at least one of the other permutations of the set.

7. A method as claimed in claim 5, wherein the linear characteristic has a probability equal to ½ in at least one of the permutations.

8. A method as claimed in claim 6, wherein $n = 4$ and $p_{lin} = ¼$.

9. A method as claimed in claim 1, wherein the set of permutations consists of two permutations.

10. A method as claimed in claim 1, including performing the selection of the permutation under control of an encryption key.

11. A method as claimed in claim 9 and 10, wherein the selection of the permutation is performed under control of one bit of the encryption key.

12. A computer program product where the program product is operative to cause a processor to perform the method of claim 1.

13. A system for cryptographically converting an input data block into an output data block; the method system including:

- an input for receiving the input data block;
- a storage for storing a predetermined set of at least two permutations associated with an S-box;
- a cryptographic processor for performing a non-linear operation on the input data block using an S-box based on a permutation; the processor being operative to, each time before using the S-box, (pseudo-)randomly selecting the permutation from the stored set of permutations associated with the S-box; and
- an output for outputting the processed input data block.